UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/673,239	09/30/2003	Masashi Morioka	243403US8	5391

22850 7590 02/28/2008

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
JOHNS, CHRISTOPHER C	

ART UNIT	PAPER NUMBER
3621	

NOTIFICATION DATE	DELIVERY MODE
02/28/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/673,239	MORIOKA ET AL.	
	Examiner	Art Unit	
	CHRISTOPHER JOHNS	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. The Applicants' amendment filed 3 December 2007 is acknowledged.

2. Applicants amended the Abstract as well as claims 1-18. Accordingly, claims 1-18 remain pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1 and 6-18 rejected under 35 U.S.C. 102(b) as being anticipated by RFC 1898, hereafter referred to as CyberCash.

As per claims 1, 15, and 16, CyberCash teaches:

5. receiving a request for usage of a service from the terminal through the information network, selecting at least one situation from plural situations each of which identifies a content network environment and a system policy, based on a description of a terminal network environment and a terminal system policy in a service certificate sent from the terminal (see sections 4.4.1 and 4.4.2 - where the credit card system either authorizes, or authorizes and charges the credit card; section 4.4, 4th paragraph, where the systems use "bypass messages" to allow merchants to obtain the credit card number, when system policy and network environment deems it necessary; also see

RFC 793, covering TCP/IP (a protocol inherently used by systems that implement both CyberCash and the present application's invention), especially section 3.1, covering the "Urgent Field");

6. changing a service procedure or a message format to operate the authentication and payment system according to the selected situation (see section 1.3 - the CyberCash server receives a request from a merchant's web server and selects the proper mode of operation from the received request and performs said operation, based on the "acquiring bank").

7. Claim 15 covers the process for the system in claim 1, and is similarly rejected.

8. Claim 16 covers the device for the system in claim 1, and is similarly rejected.

9. **As per claim 6, CyberCash teaches:**

10. a receiver configured to receive a request for a service including a certificate of service sent from a terminal through an information network (CyberCash's server receives a certificate from the merchant's server through the Internet – see section 1.3, 2nd paragraph);

11. a controller configured to select a timing of providing the service in response to the request for the service from the terminal (the TCP/IP protocol, inherently used to enable the system described in CyberCash, allows for congestion control that lets computers determine when to send data – as a reference, see RFC 2581 (sections 3.1 and 3.2 especially));

12. a transmitter configured to transmit a request for authentication and payment with or without a digital signature to an authentication and payment device through the information network, wherein the request for authentication and payment is formed from all or a part of the certificate of service or from all or a part of the certificate of service and additional information (CyberCash interprets the certificate and "forwards the relevant information to the acquiring bank" (See section 1.3, 2nd paragraph), using encryption (See section 1.2). Also see section 2.1, item #3 and section 2.5; the Opaque portion of the data is not always sent - it depends on the situation at hand).

13. **As per claim 7, CyberCash teaches:**

14. the request for authentication and payment is formed from identification information including at least one of an identifier of the certificate of service, an identifier of the authentication and payment device and a digital signature of the authentication and payment device, which are extracted from the certificate of service, or from the identification information and the additional information and the request for authentication and payment is transmitted with or without a digital signature (said request for authentication and payment includes the identification information of the customer (See section 1.3, 1st paragraph) and relevant merchant information (See sections 1.3, 1st paragraph; 4.3.2, "merchant-ccid" and "transaction"; 4.4.1, "merchant-ccid", "merchant-transaction", "merchant-date", and "merchant-cyberkey"; 4.4.2, "merchant-ccid", "merchant-transaction", "merchant-date", and "merchant-cyberkey").

15. **As per claim 8, CyberCash teaches:**

16. a controller configured to select timing of processing the request for authentication and payment to the authentication and payment device, and configured to simplify the processing of the request for authentication and payment (CyberCash enables merchants and banks to "more quickly integrate safe on-line payments into their existing service offerings" (See section 1.1, 1st paragraph).

17. **As per claim 9, CyberCash teaches:**

18. another receiver configured to receive a first certificate of service from the terminal through the information network, and another transmitter configured to generate a second certificate of service by adding the additional information to the first certificate of service and to transmit the generated second certificate of service to the terminal through the information network (said second "receiver" and second "transmitter" for sending the "generated second certificate" to the terminal are both included in CyberCash (See the CH2 message in section 4.3.3)).

19. **As per claim 10, CyberCash teaches:**

20. a certificate of service issuing unit configured to issue a certificate of service to an other device, the certificate of service indicating a maximum number of times the certificate of service may be used (see section 4.4.6, for the CM6 message sent from the server to a merchant. Certificates implicitly indicate the maximum number of uses, since they inherently may only be used once, because of the existence of session data

such as in CM1, in section 4.4.1 – CM1 contains "merchant-transaction", "cyberkey", and the opaque section, all of which are single-use);

21. a processing unit configured to process at least one of verification of a request for authentication and payment sent from the other device through an information network, authentication of the received request for authentication and payment, permission for provision of a service that is requested by the request for authentication and payment, and payment for the provision of the service (see section 4.4.1, for the CM1 message sent from the merchant to the server).

22. **As per claim 11, CyberCash teaches:**

23. the certificate of service contains at least one piece of information of an identifier of the certificate of service, an identifier of the authentication and payment device, an identifier of the other device, information of expiration date of the certificate of service, and information of a constraint of the service to the other device (The server in CyberCash contains all of these features. The CM6 message (cf. section 4.4.6) contains: the "transaction" and "merchant-transaction" fields ("at least one piece of information of an identifier of the certificate of service"), the "merchant-ccid" field ("an identifier of the other device"), an "expiration-date" field which determines the expiration of the credit card, effectively expiring the certificate as well, since it would no longer be valid after the expiration date ("information of expiration date of the certificate of service"), and the "action-code" field, which (per ISO 8583) is a standard for financial transactions – the field represents what sort of action has taken place; e.g.

authorization, payment, reversal ("information of constraint of service to the other device"). Additionally, because CyberCash is designed for the Internet, the IP header in the packet data containing the CM6 message would contain the server identification information e.g.: the server's IP address ("an identifier of the authentication and payment device")).

24. **As per claim 12, CyberCash teaches:**

25. an information storing unit configured to store all or a part of information to be contained in the certificate of service as a stored information, wherein the certificate of service includes information of a location of the stored information in the information storing unit (CyberCash's server stores a database of transactions for auditing purposes – see section 4.4, 4th paragraph, which states that obtaining information pertinent to dispute resolution is an "auditable event". For dispute resolution, a merchant would need specific information about the transaction event. By referencing the transaction event using the transaction number, contained in the certificate of service, as well as "special bypass messages", the merchant can obtain necessary dispute resolution information).

26. **As per claim 13, CyberCash teaches:**

27. a transmitter configured to transmit the certificate of service to the other device in response to a request from the other device or in accordance with a predetermined

condition for transmission (CyberCash's server may send a CM6 message – "given to the merchant as a receipt for a completed charge action"; see section 4.4.6).

28. **As per claim 14, CyberCash teaches:**

29. the certificate of service issuing unit is further configured to update a content of the certificate of service based on updated information under control of the authentication and payment device, and the transmitter transmits the updated certificate of service to the other device (CyberCash's service will respond with the CM6 message retaining some information from the CM1/CM2 message (e.g. "transaction") but updating and adding new information (e.g. "response-code" and "authorization-code"). (These messages are covered in sections 4.4.1, 4.4.2, and 4.4.6)).

30. **As per claim 17, CyberCash teaches:**

31. an opening unit configured to open the control information generated by the control information generating means to the information network (in order to process control information, any computer inherently must "open" the information).

32. **As per claim 18, CyberCash teaches:**

33. the control information includes information of an identifier (CyberCash's server will receive a request for service and create control information based on said request. This request (such as the CM1 message in section 4.4.1) will contain identifying information about the customer, which the server will correlate to bank information and

send a request to the banking system associated with said account (see section 1.3, 2nd paragraph)).

34. Claims 2-4 rejected under 35 U.S.C. 102(b) as being anticipated by US Patent 5,870,473 (hereafter referred to as Boesch).

35. **As per claim 2, Boesch teaches:**

36. a receiver configured to receive a first certificate of service including information from an authentication and payment device and a digital signature through an information network (see claim 17 of Boesch: the terminal "[receives] said invoice including said portion of the terms of the transaction from said merchant device and [transmits] said portion of said customer response to the merchant device". The merchant device has received the "session" from the server, and transmits a certificate to the customer device, "including at least a portion of the terms of the transaction". Digital signatures are used in the invention to "authenticate information" (column 29, lines 50-55, among others));

37. a transmitter configured to generate a second certificate of service based on the first certificate of service, the second certificate of service including identification information of the terminal, and to transmit the second certificate of service to a service providing device through the information network (the terminal will send the "portion of [the] customer response" to the merchant device. Since this invention is designed for

Internet commerce, terminal information will be sent along with the "customer response", e.g. an IP address).

38. **As per claim 3, Boesch teaches:**

39. The second certificate of service is generated from all or a part of the first certificate of service; from all or a part of the first certificate of service and additional information; from all or a part of the first certificate of service and the digital signature; or from all or a part of the first certificate of service, the additional information and the digital signature (see claim 17 of Boesch: the second certificate sent to the service providing device is generated from "a part of the first certificate of service").

40. **As per claim 4, Boesch teaches:**

41. the second certificate of service is generated from identification information including at least one of an identifier of certification, an identifier of an authentication and payment device, and a digital signature of the authentication and payment device, which are extracted from the first certificate of service, from the identification information and the additional information, or from the identification information: the additional information, and a digital signature (the second certificate sent to the service providing device is generated from the "identification information" of the terminal's user (since the transmission occurs over the Internet, identification information of the terminal is sent in the IP header of the datagrams which contain the certificate) and a "piece of new information" like the "note-hash" (See Figure 28A, row 5113F).

Claim Rejections - 35 USC § 103

42. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

43. Claim 5 rejected under 35 U.S.C. 103(a) as being unpatentable over CyberCash, in view of Official Notice.

44. **As per claim 5, CyberCash teaches:**

45. usage history managing unit configured to manage a usage history of a certificate of service distributed from an authentication and payment device through an information network (CyberCash is a "stateful" protocol – that is, the protocol has a "memory" or "state" and follows a pre-defined set of steps based on the data received and sent. (Compare to "stateless" which means that each transaction takes place independent of any previous ones.) At each point, the customer device ("terminal") knows where it is in the process and is waiting for a specific message to be sent. By its nature, a stateful protocol may be rolled back – if there is an error, or for logging purposes, one can follow the steps backwards to understand what has occurred

46. Additionally, the Examiner takes Official Notice that storing a usage history for logging (and other) purposes was well-known to those skilled in the art at the time of the invention. Web browsers were well-known to those skilled in the art at the time of the

invention to store a 'cache' of past-visited webpages, in order to provide a history of visits, as well as faster access to said webpages);

47. the usage history including information regarding at least one previous transaction (CyberCash does not directly teach that the usage history contains at least one previous transaction. The Examiner takes Official Notice that storing a usage history is old and well-known to those skilled in the art at the time of the invention – web browsers were well-known to store a "cache" of visited webpages, in order to provide a history of visits and faster access to often-visited pages. Both web browsers and CyberCash are drawn to the field of electronic communication, where past actions are stored in electronic history systems. It would be advantageous to store the usage history in CyberCash in a usage history system such as the one in web browsers, because of the ease of auditing the CyberCash system (something stated to be desired in CyberCash; see section 4.4, 2nd to last paragraph). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to add the history management system in web browsers to the system in CyberCash);

48. an acknowledgement unit configured to acknowledge to the authentication and payment device when the usage history satisfies conditions defined in the certificate of service (CyberCash allows the terminal to acknowledge to the server (which acknowledges to the "authentication and payment device") when it "satisfies conditions defined in the certificate of service" – it sends the CH1 message to the merchant with payment information, see section 1.3, 1st paragraph).

49. Claims 1, 6, 15, and 16 rejected under 35 U.S.C. 103(a) as being unpatentable over CyberCash, in view of Request For Comment 793, further in view of Request For Comment 2581 (documents that detail Internet standards and protocols).

50. **As per claims 1, 15, and 16, CyberCash teaches:**

51. receiving a request for usage of a service from the terminal through the information network, selecting at least one situation from plural situations each of which identifies a content network environment and a system policy, based on a description of a terminal network environment and a terminal system policy in a service certificate sent from the terminal (see sections 4.4.1 and 4.4.2 - where the credit card system either authorizes, or authorizes and charges the credit card; section 4.4, 4th paragraph, where the systems use "bypass messages" to allow merchants to obtain the credit card number, when system policy and network environment deems it necessary.

52. Alternatively, if not inherent, see RFC 793, covering TCP/IP (a protocol used by systems that implement both CyberCash and the present application's invention), especially section 3.1, covering the "Urgent Field". It would have been obvious to use the device for Urgency in order to control system flow and to communicate system policy and network environment – namely that the packets sent by that system were of an urgent nature and should be processed quickly – because of the desire to prioritize different network activities, depending on the urgency of such activities. The system described in CyberCash was designed to "quickly…transport payment between buyers, sellers, and their banks" (see section 1, 1st paragraph), and TCP/IP would enable the

speed to be attained. Additionally, CyberCash is implemented on top of the normal Internet, which uses the TCP/IP protocol to communicate);

53. changing a service procedure or a message format to operate the authentication and payment system according to the selected situation (see section 1.3 - the CyberCash server receives a request from a merchant's web server and selects the proper mode of operation from the received request and performs said operation, based on the "acquiring bank").Claim 15 covers the process for the system in claim 1, and is similarly rejected.

54. Claim 16 covers the device for the system in claim 1, and is similarly rejected.

55. **As per claim 6, CyberCash teaches:**

56. a receiver configured to receive a request for a service including a certificate of service sent from a terminal through an information network (CyberCash's server receives a certificate from the merchant's server through the Internet – see section 1.3, 2nd paragraph);

57. a controller configured to select a timing of providing the service in response to the request for the service from the terminal (It is the examiner's primary position that the claims are anticipated because of inherent features (i.e. the timing selection being performed by the TCP/IP stack on a computer system). However, if not inherent, the TCP/IP protocol directly teaches congestion control that lets computers determine when to send data – as a reference, see RFC 2581 (sections 3.1 and 3.2 especially). It would have been obvious to one of ordinary skill in the art at the time of the invention to use

the congestion control mechanism in TCP/IP because of the ability to control the traffic on a network and properly time sending of data. This enables, as described in CyberCash, a way through which "payments can be transported quickly, easily, and safely between buyers, sellers, and their banks" (see section 1, 1st paragraph));

58. a transmitter configured to transmit a request for authentication and payment with or without a digital signature to an authentication and payment device through the information network, wherein the request for authentication and payment is formed from all or a part of the certificate of service or from all or a part of the certificate of service and additional information (CyberCash interprets the certificate and "forwards the relevant information to the acquiring bank" (See section 1.3, 2nd paragraph), using encryption (See section 1.2). Also see section 2.1, item #3 and section 2.5; the Opaque portion of the data is not always sent - it depends on the situation at hand).

Response to Arguments

59. Applicants' arguments filed 3 December 2007 have been fully considered but they are not persuasive.

60. As for the argument that "CyberCash fails to teach or suggest a service certificate sent from the terminal (e.g., internet customer) that identifies a network environment or a system policy" and that "CyberCash fails to teach or suggest selecting a situation that identifies a network environment or a system policy", the Applicants should note that the TCP/IP system allows data to indicate the environment and policies that are present. Additionally, CyberCash also discloses, in sections 4.4.1 and 4.4.2,

different situations and different data being sent to indicate different network and system policy situations.

61. As for the argument that "CyberCash fails to teach or suggest changing a service procedure or a message format according to the selected situation", the Applicants should note that in sections 4.4.1 and 4.4.2, different situations and different data are sent to indicate different network and system policy situations.

62. In response to Applicants' argument that CyberCash fails to teach or suggest "a usage history managing unit configured to manage a usage history...", where the Applicant argues that CyberCash differs from the present application because of the idea of lump payments and how the history of such payments would function in the system, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

63. As for the arguments on pages 16 and 17 that Boesch et al "teaches away from using digital signatures", Applicants are directed to the following: column 29, lines 50-55, column 32, lines 34-45, column 34, lines 34-48, column 42, lines 25-33, column 51, lines 32-46, column 61, lines 18-26, and column 77, lines 1-8. Clearly Boesch et al teaches using digital signatures - and does not, in fact, "teach away" from using them.

Conclusion

64. Applicants' amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicants are reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

65. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

66. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER JOHNS whose telephone number is (571)270-3462. The examiner can normally be reached on Monday - Friday, 9 am to 5 pm.

67. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on (571) 272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

68. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CHRISTOPHER JOHNS
Examiner
Art Unit 3621

CCJ

/Bradley B Bayat/
Primary Examiner, Art Unit 3621